Remarks

Reconsideration is requested in view of the preceding amendments and the following remarks. By this Amendment, claims 1, 7, 15, 23, and 30 are amended, and claims 6 and 31 are cancelled without prejudice. Upon entry of this Amendment, claims1-5, 7-30, and 32-38 are in the application.

Claims 1-23 and 27-38 stand rejected as allegedly anticipated by Bernhard et al., U.S. Patent 6,275,942 ("Bernhard"). This rejection is traversed. The pending claims are directed to improved intrusion detection. Bernhard teaches automatic response modules (ARMs) for responding to computer misuse such as intrusions, but Bernhard does not teach or suggest any of the claimed intrusion detection methods or apparatus. Bernhard's ARMs are configured to provide flexible responses to computer misuse in order to counter or fix problems arising from detected misuse. Col. 2, lines 17-21. According to Bernhard, a real-time reaction to computer misuse is needed, not a mere notification of an intrusion. Col. 2, lines 25-34 (emphasis added).

For example, claim 1 as amended recites a method for implementing an intrusion detection system that includes "receiving a request at a software agent program to initiate intrusion detection services on a remote computer, wherein the request is issued in response to a notification of a network intrusion." Bernhard does not teach or suggest such a method. While Bernhard does teaches notification of a network intrusion, Bernhard teaches activating ARMs to respond to the intrusion in order to, for example, prevent access from an IP address associated with an intrusion (a "firewall" ARM), disabling a user account (a "Kerberos" ARM), or respond to file corruption or deletion (a "fix-it" ARM). Bernard discusses these and other types of ARMs at, for example, col. 8, line 47 to col. 10, line 10. Bernard does not teach or suggest initiating intrusion detection based on a notification of an intrusion. Therefore, claim1 and dependent claims 2-5 and 7-14 are properly allowable.

Claim 15 as amended recites a method for implementing an intrusion detection system that comprises, in part, receiving a request to become an intrusion detection platform from a remote network location, wherein the request is issued in response to a notification of a network intrusion. Bernhard does not teach or suggest such as method. Bernard teaches ARMs for countering of fixing problems associated with computer misuse, and does not teach or suggest implementing intrusion detection based on a notification of an intrusion. Therefore, claim 15 and dependent claims 16-22 are properly allowable.

Claim 23 as amended recites a system for detecting intrusions in a computer network. The system comprises a database configured to store at least one rule defining as least one response to a network intrusion, and an intrusion detection server that sends a request to execute intrusion detection software to a software agent at at least one of a plurality of computers when intrusion detection services are needed based on the at least one stored rule. While Bernhard teaches intrusion detection, Bernhard does not teach or suggest requesting execution of intrusion detection software based on a rule defining an intrusion response as stored in a database. Bernhard's ARMs are directed to particular responses to particular intrusions to counter particular problems, and not merely increasing, decreasing, or otherwise configuring intrusion detection services. Therefore, claim 23 and dependent claims 24-29 are properly allowable.

Claim 30 recites an article of manufacture comprising a computer-readable medium having stored thereon instructions that define a series of steps to be used to perform network intrusion detection. The instructions comprise receiving notification of a network intrusion and installing intrusion detection software on a remote computer via a software agent program in response to the received notification. Bernard does not teach or suggest installing intrusion detection software in response to a notification of a network intrusion, but instead teaches ARMs that are targeted to counter

or fix problems associated with a particular type of intrusion. Col. 2, lines 25-34. Therefore, claim 30 and dependent claims 32-38 are properly allowable.

Claims 24-26 stand rejected as allegedly anticipated by a combination of Bernhard and Gaisford et al., U.S. Patent 6,023,586 ("Gaisford"). This rejection is traversed. Claims 24-26 depend from allowable clam 23 and are therefore allowable for at least this reason.

In view of the preceding amendments and remarks, all pending claims are in condition for allowance and action to such end is requested.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

By _____
Michael D. Jones
Registration No. 41,879

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446